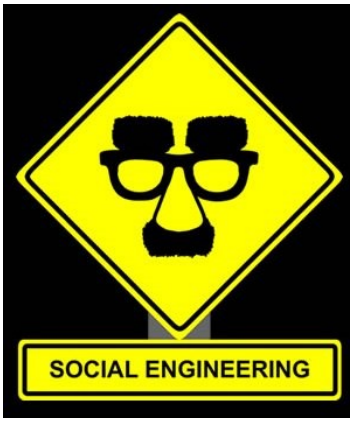
SITSD
Enterprise Security Program

Security Matters

Welcome to the inaugural issue of Security Matters, the monthly information security newsletter published by the Enterprise Security Program. Along with the newsletter, we've attached a file with material you can use to promote information security awareness each month. We hope you'll find the newsletter and materials useful and hope you'll give us feedback on what we can do better. Your suggestions for topics and content are welcome. Contact us.

Focus on Social Engineering

Social engineering has been used for millennia even if the phrase "social engineering" is a more recent one. One of the most infamous social engineering feats involved a city with impregnable walls, an army intent on conquering the city, a long-standing siege, and a very large horse. It's no coincidence that malicious software that looks harmless in order to trick people into installing it and then attacks the device is called a "Trojan Horse".



So what exactly is social engineering? **Social engineering is manipulating a person to do things that he or she would not have otherwise done. It uses psychology as much as technology to achieve a goal – and sometimes doesn't use technology at all.** While it can be used in some settings for good, we generally consider social engineering to be one of the greatest threats to security that organizations face today.

Phishing and its phishy cousins. Some social engineering is familiar by other names. Most people know about phishing (and the variations of spear-phishing and whaling) which is a kind of social engineering that involves the use of a legitimate-looking email to trick the recipient into allowing malicious software to be installed or to provide confidential information such as account numbers and passwords.

Don't be frightened by scareware. Scareware is a tool malicious actors use to frighten people into installing and/or running software. If you've ever seen a pop-up when surfing the internet that warns you your anti-virus is out of date, that a virus has been

Continued on page 5

National Cyber Security Awareness Month

October 1 marks the start of the 12th annual National Cyber Security Awareness Month (NCSAM). Started in 2004 was started as a partnership between the U.S. Department of Homeland Security (DHS) and the National Cyber Security Alliance with the goal of raising awareness about cyber security. We live increasingly connected lives and more than ever cyber security is vital to protecting our identities, our finances, our businesses, and our safety.

The Enterprise Security Program (ESP) has signed on as a NCSAM Champion as well as a member of the Stop.Think.Connect Cyber Awareness Coalition. Beginning in October 2015 the ESP will be holding security awareness events with activities, informational handouts, treats, giveaways, and prizes. The events will continue throughout the year. With each month focusing on a different topic. See page 3 of this newsletter or visit the Montana Information Security website for the most current list of Security Awareness Events.

Inside this issue:

A monthly update on the latest security threats.

- Sean Rivera, CISSP

Current Threats and Vulnerabilities

Vulnerability in iPhones

In September, a vulnerability in Apple's AirDrop file-sharing program came to light as it was revealed that an attacker could wirelessly send a malicious program to an unsuspecting victim via Bluetooth. This vulnerability also exists on Apple Mac computers with AirDrop enabled as well. The good news is that the vulnerability has been fixed, and Apple strongly recommends users upgrade to the latest versions of iOS and Mac OS after users perform sufficient backups of their data.

Telephone Scams Make a Surge in Montana

A recent wave of Vishing (Voice-phishing) has been targeting Montanans posing as tech support providers. Targets receive a phone call from an individual claiming to be some form of tech support for a major vendor stating that their system is infected with a virus. The scam goes on in an effort to manipulate the target to install malicious software in an effort to commit ID theft and other nefarious actions. Users should be made aware that software and hardware manufacturers do not make these types of cold-calls. Also, users should be encourages to never provide any personally identifiable information or any account numbers to anyone with whom they did not initiate the call.

Meeting Highlights of the Montana Information Security Advisory Council Meeting & Preview of the Upcoming Meeting

Meeting highlights from September 16, 2015

The MT-ISAC has voted to accept the Five Enterprise Security Framework Policies based on NIST Cyber Security Framework. Agencies will work toward compliance in a three year period, not to exceed five years with yearly status updates from each agency.

The Appendix A (Baseline Security Controls) of the Information Technology Security Risk Management Policy were also accepted. This updated version consolidated twenty eight Enterprise Security Polices/ Standards/Procedures within the Baseline Security Controls.

The MT-ISAC Goals and Objectives for the 2015 Biennium were also accepted.

A report of the Department of Revenue (DOR) Joint Task Force on Fraud and Identity Theft meeting on September 1, 2015 was given. If interested in joining the Task Force, please contact Lynne Pizzini, Margaret Kauska, or Lee Baerlocher.

The SITSD Enterprise Security Program (ESP) presented on cybersecurity awareness activities for October 2015-September 2016. The theme for the year will be "Stay Safe on the Information Highway".

Looking to the October 21, 2015 Meeting

The SITSD Enterprise Security Program will map the Appendix A (Baseline Security Controls) back to the five Enterprise Security Framework Policies. This will aid agencies in the work toward compliance.

Formation of MT-ISAC workgroups will be discussed. The focus of these workgroups will be to accomplish the newly passed MT-ISAC Goals and Objectives.

For more information, visit the MT-ISAC website.

Get Involved in NCSAM

#CyberAware is the hashtag for the month – join in the conversations already happening online.

The NCSAM Planning Guide includes template articles, social media posts, and a list of daily ideas.

NCSAM and Stop.Think.Connect. 5th Anniversary Logos for your materials and website.

NCSAM Weekly Themes provide more information on the cyber-related topics for the month.

Promote your event on the NCSAM calendar.

Sign up as a NCSAM Champion. It's free and takes only a few minutes.

Host a security awareness event at your office. For more information contact Lisa Vasa.

MS-ISAC 2015 National Cyber Security Awareness Month Toolkit Posters, 2016 calendar, and other resources for promoting cyber security awareness

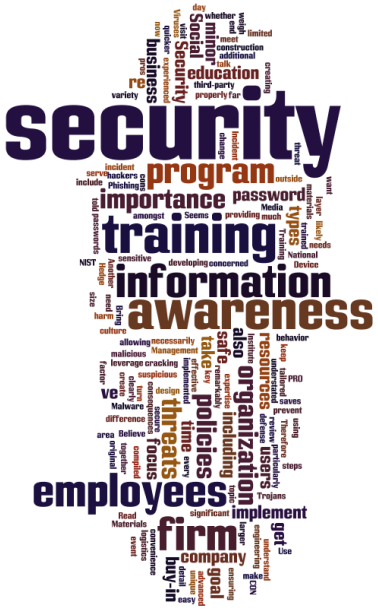
October 2015 Events

Focus on Social Engineering

- Oct 8, 2015 - 2:00-4:00 p.m. at the State of Montana Data Center - Helena
- Oct 14, 2015 - 10:30-2:00 at the Mitchell Bldg., Room 53
- Oct 21, 2015 - 11:00-4:00 at the Capitol Rotunda
- Oct 22, 2015 - 10:30-2:00 at the Cogswell Bldg., Room TBD
- Oct 27, 2015 - 10:30 - 2:00 at the Mitchell Bldg., Room 53

Check **Montana Information Security** for the latest event schedule.

Security Training News



SANS Securing the Human End User Training

All user training records in the SANS Securing the Human system have been reset to start the 2015-2016 training year. Users who did not complete training in 2014-2015 have been archived and removed.

Each agency should take time to review and make any training policy updates or changes needed for the upcoming year. Agencies should also check for any personnel who may have been accidently dropped in this process or are new since the transition and make additions as needed. This will allow everyone to start the training year with a current plan.

The Enterprise Security Program (ESP) has recommendations for training policies for the next two years available on the Montana Information Security website. These recommendations are based on a set of Core modules that are critical information for all users with additional modules for 2015-2016 and different modules for 2016-2017 to provide some variety in the training. This training in total is approximately one hour. There are also recommended modules for meeting specific compliance or job-related requirements.

The ESP is happy to work with agency administrators to create training policies that meet the needs of the agency. To request assistance, please open a case with the SITSD Service Desk at 444-2000 or online.

Security Training Resources

Making Sense of Threat Reports

Webinar sponsored by Solar Winds—October 21, 2015 1:00-2:00 ET

We'll be exploring various threat reports and will discuss the most important things you can do to keep your networks and data safe. More information and registration.

State and Local Cybersecurity: A Guide to Federal Resources

Virtual Event — November 12, 2015 11:00– 2:00 ET

Watch from your computer as a panel of cybersecurity experts from NIST, GSA, and DHS provide state and local officials with a better understanding of how to take full advantage of NIST, FedRAMP, and CDM programs. Registration is FREE for government and military personnel. More information and registration.

Federal Virtual Training Environment (FedVTE)

Just when you thought we were teasing about the FREE courses available, we'll tell you about the FedVTE cybersecurity training system. Courses range from beginner to advanced levels and are available at no cost to users. Sign up is easy at: www.Fedvte.usalearning.gov and a catalog of available courses is on the site.

National Incident Management Systems (NIMS)

The FEMA NIMS training program provides a common approach for managing incidents with a number of courses designed to meet specific incident management needs. Visit the NIMS website for more information.

For more security training and awareness resources, check out the Security Training Resources page and watch for more information here each month.

Focus on Social Engineering (continued from Page 1)

detected, or other problems exist on your computer, that is scareware.

Phone tactics, also known as Vishing. Using scare tactics to manipulate people can also be done over the phone. Would-be identity thieves and scam artists call people on the phone and use various scenarios to get the person to provide personal information or to give them money. For example, the caller may say that your credit card account has been compromised and in order to keep it from being suspended, you need to provide the caller with your account number and other details. Another common scam is a call about your computer being infected or in need of updates. The caller instructs the person to go to a website and download software to fix the problem.

You're a winner! Sometimes the con is the opposite scenario – something great is in store if you'll just do a few things or provide some information. You've won the lottery and all you have to do to collect is send a small processing fee. You're the lucky recipient of an all-expenses-paid dream vacation. In order to prepare the trip arrangements you're asked for personal details like your birthday, address, driver's license number, and/ or passport number.

Social engineering takes advantage of our natural inclination to want to help. The request might be in the form of a phone call asking to have a password reset for a system for which you have the authority to do so. It might be a person who knocks on the door or is standing outside an office building who says he forgot his access badge or has a meeting with someone in the building. It may be a "tech support" person who is there to fix a problem – a problem that doesn't exist, but makes a great excuse for accessing a restricted space.

With all the methods that scam artists may use to manipulate us, it's easy to see why so many social engineering attacks are successful and why it's hard to defend against them.

Your best defense is to always stay alert and question anything that seems even a little bit off. Here are some more specific suggestions to help prevent you from being a victim of social engineering:

If you see an unaccompanied, unfamiliar person in your work area, ask and verify his identity and purpose for being there. Some ways to verify are by examining his ID, calling another person who can vouch for him, or checking with your supervisor. But remember, if he claims to work for XYZ Company and offers you a phone number for them to check on him, you may wish to obtain the number from an independent source to be safe.

Remember banks and other financial institutions will not call you and ask for personal and account information over the phone. When in doubt, tell the caller you'll call them back and call the phone number from your account statement or other documents, rather than the caller. NEVER give out social security numbers, account information, and/or passwords over the phone to an unsolicited caller.

Likewise, unexpected callers who claim to be from Microsoft or other tech companies are also frauds. If you have not contacted a company for assistance with a problem, do NOT provide personal information or install software at the request of a person claiming to be technical support. Remember, software manufacturers NEVER call users to fix viruses or apply updates.

If it sounds too good to be true it probably is. Who wouldn't love to win a big prize? But if you didn't enter, you won't win. And even if you did enter and win, you wouldn't be required to pay to collect your winning. Neither would you be required to provide your bank account information

Don't fall for the scare or intimidation tactics either. Your grandson is not in jail in Mexico and needing money immediately. Your credit card isn't on the verge of being suspended. If you think either of those cases *might* be true, verify the information by trying to personally contact the person allegedly in trouble or by calling your financial institution directly. We can't stress it enough – NEVER provide personal, confidential, or financial information to an unknown caller.

In the office, establish policies for responding to requests such as password resets and physical access. Make sure staff members know and follow the policies.

Last of all, speak up if you experience something you think may have been an attempt to commit fraud or cause harm. At the office, report the event to your help desk or security team. At home, contact local law enforcement or the Department of Justice's Office of Consumer Protection.

Social engineering is a huge threat, but we can beat it if we all do our part. Stay aware, don't share sensitive information over the phone or via email without verifying with whom you're sharing it, don't install software or visit unfamiliar websites when requested by a stranger, and don't assume that what people tell you is always the truth.

When it comes to social engineering, skepticism may be your best friend.

News You Can Use

Focusing on Social Engineering

Are your fingerprints, email and image worth a cute fake passport?

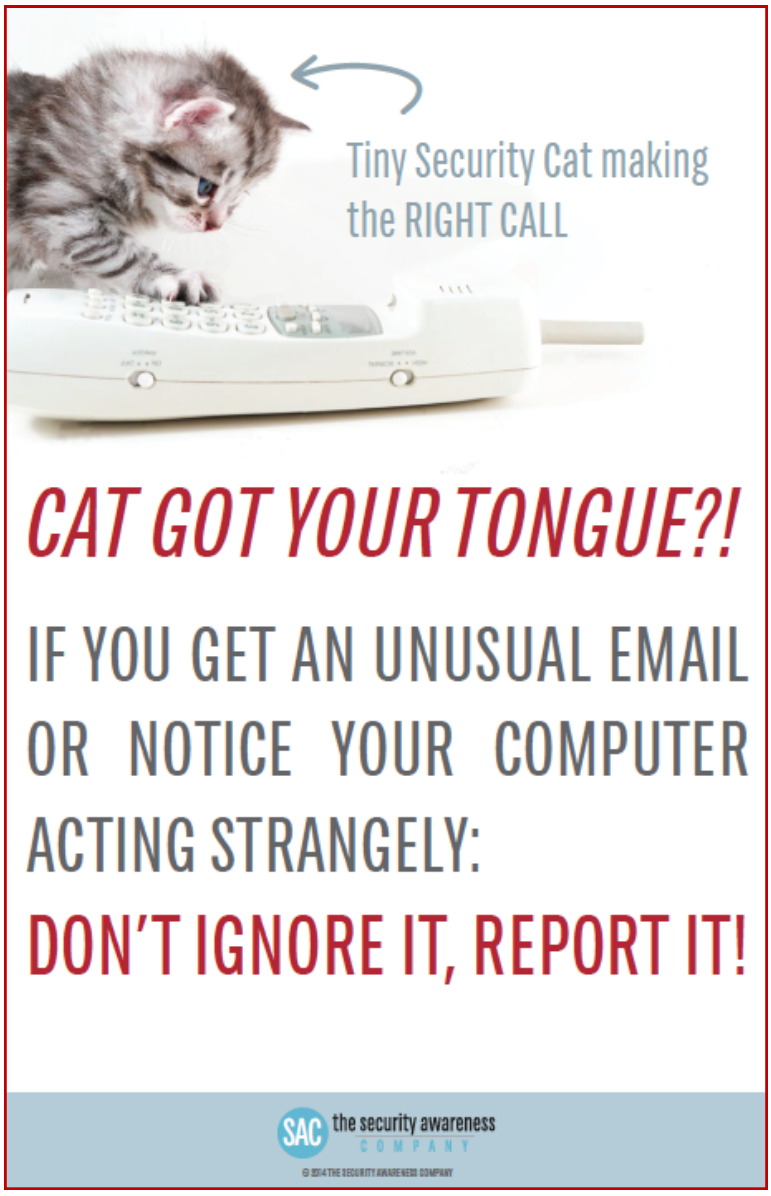
Lisa Vaas of the Sophos blog Naked Security gives a demonstration of how easily we give up private information for the sake of games and online fun.

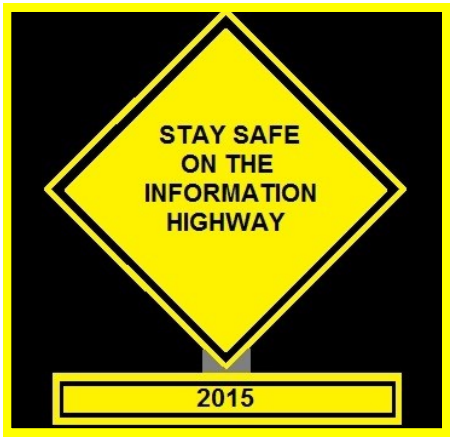
The 7 Best Social Engineering Attacks Ever

Dark Reading's Sara Peters has seven reminders of why technology alone isn't enough to keep you secure.

Hey Scandos, missed that parcel? Here's some ransomware instead

Spam emails disguised as messages from the local post office or other delivery services are serving up ransomware. This article by John Leyden





Security Quick Tip

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking for your personal or financial information. NEVER provide personal or financial information in emails, including links sent in emails.

For more security tips, news, advisories, and resources visit the Montana Information Security website:

http://sitsd.mt.gov/MontanaInformationSecurity

Contact Us:

Enterprise Security Program

Lynne Pizzini, CISO and Deputy Chief Information Officer

Joe Frohlich, Enterprise Security Manager